REMARKS

Applicants gratefully acknowledge the examiner's indication that the prior art rejections of claims 14-28 had been withdrawn and that claims 23, 24, and 26-28 are directed to allowable subject matter. However, Applicants respectfully traverse the indefiniteness rejections as follows:

The objection to claim 25

Claim 25 has been amended to address the informality noted by the examiner.

The rejection of claims 14-22 under 35 USC 112, second paragraph, as being indefinite

Applicant respectfully notes that the office action has misinterpreted Applicants' sentence on page 22, lines 8-12. As indicated by the title to the application, claim 14 is directed to a "block-level" storage device. As discussed on page 6 of the specification, many conventional storage engines are block-level devices – examples include hard disk drives in PCs and DVD drives. Host systems that interface with such storage devices must translate a file request to the actual physical addresses for the corresponding blocks of data on the storage medium that is accessed by the storage engine.

Applicants disclosed an advantageous block-level DRM technique in which the host system accessed both the data and its metadata using block-level requests. However, as discussed on page 20 of the specification, the host system may be vulnerable to hacker attack in such embodiments because the host is in complete control of the data/metadata linkage. Thus, Applicant proposed an alternative embodiment in which the storage engine itself has some control over this linkage with respect to, for example, copy rights and unlocking operations. As discussed on page 20, lines 15-18, the storage engine gains such control through the addition of a "security repository" to the storage medium. As set forth, for example, on page 20, lines 23-25, the security information in this repository applies to file system objects rather than to block addresses. Claim 14 reflects such a repository by reciting "a storage medium configured to store security metadata for the secure file system objects."

An example write operation is discussed beginning on page 21, line 10 with respect to a host requesting the storage engine to write a file denoted as "myfile.text' to the storage medium. The host encrypts this file such that it is encrypted and associated with the corresponding security metadata. Applicants proposed that the block addresses for this example file correspond to block addresses 1 through 10 on the storage medium. Thus, the host system transmits block write requests to the storage engine such that the encrypted content is written to block addresses 1 through 10 on the storage medium. Because this file is encrypted, the host system also transmits the security metadata to the storage engine. In the first embodiment described by the Applicants (in which the storage engine does not control a security repository), the storage engine would not be aware of the linkage between the security metadata associated with block addresses 1 through 10. However, in the "smart" second embodiment, the storage engine knows that the security metadata applies to a file system object rather than just to block addresses. However, as noted by the title of the application, the host is still using a block-level driver and requesting the data (as opposed to the metadata) using block-level requests. That the host still requests the data using a block-level driver is made explicit on page 23, line 20-25, where the Applicants state: "What is important is that the host system 25 be configured to interact with the security repository on a file system object level rather than the block level it uses to access the encrypted content on disc 23."

In that regard, it is noted that citation on pages 3-4 of the office action to the sentence on page 22, lines 8-12 of the specification is not inconsistent whatsoever with what is recited in claim 14. Specifically, this sentence contrasts the "SECURE_READ_FILE_SYSTEM_OBJECT" command in the embodiment in which the storage engine has knowledge that the security metadata applies to a certain file system object as opposed to the first-described embodiment in which the storage engine has no such knowledge and responds to a "SECURE_READ_BLOCK" command. In both cases, the host system addresses the data (as opposed to the security metadata) on a block-level. For example, the block-level access in the first embodiment is described on page 11, lines 11-12 wherein the host transmits requests for access to blocks.

This same request occurs with the "SECURE_READ_FILE_SYSTEM_OBJECT" command except that the security metadata is linked to its data on a file-system-object level as opposed to block-level. But the content access (as opposed to the security metadata access) is always block-level in both embodiments as distinctly described on page 21 with respect to example block addresses 1-10 and also made explicit on page 23 in lines 20-23.

Applicants respectfully note that the command name "SECURE_READ_FILE_SYSTEM_OBJECT" may have been more appropriately denoted as "SECURE READ BLOCK COMMAND IN CONJUCTION WITH ACCESS TO FILE SYSTEM LEVEL METADATA" but as noted by the Applicants on page 23, lines 19-20, the command name and format is rather unimportant.

Applicants respectfully note that the sentence on page 22, lines 8-12 would better support the indefiniteness rejection if it was re-worded to end with "except that the SECURE_READ_FILE_SYSTEM_OBJECT command corresponds exclusively to a set of security metadata that applies to a file system object." But Applicants did not use the word "exclusively" and make it plain throughout their specification as discussed above that they are addressing a host system that accesses content through a block-level driver. So that sentence cannot be read to mean that the command only concerns a set of security metadata – instead, the sentence is read to mean that the command is just like the previously-described block-level write command except for the security metadata linkage (that is to say file-system-object-level linkage) by the storage engine through the security repository. Because this sentence in no way contradicts but instead supports claim 14, claim 14 is definite. Claims 15-22, being dependent on claim 14, are definite for at least the same reasons.

CONCLUSION

For the foregoing reasons, Applicants respectfully submit that the pending claims are in condition for allowance.

If the Examiner has any questions or concerns, a telephone call to the undersigned at (949) 752-7040 is welcomed and encouraged.

Certificate of Facsimile Transmission

I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date shown below.

Jonathan Hallman
Date of Signature: November 20, 2008

Respectfully submitted,

Jonathan W. Hallman
Attorney for Applicant(s)
Reg. No. 42,622
Customer No. 32,605